IN THE CLAIMS

This listing of claims replaces all prior versions:

1. **(Currently Amended)** An apparatus for providing a security status of an on-line service, comprising:

a web page object that is automatically rendered by a browser when a visitor uses the browser to access one or more web pages of the on-line service via a public network; and

a verification service that hosts the web page object separately from the one or more web pages of the on-line service, and further controls contents of the web page object,

wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status through the automatic rendering of the web page object by the visitor's browser, and

wherein the verification service causes the contents of the web page object to be ~~automatically rendered and displayed~~ changed in accordance with its prior determination of a level of the security status, such that when the verification service determines, in a first verification operation prior to the visitor's access request, that the on-line service has a first level of the security status, it causes the web page object to have first contents, and when the verification service determines, in a second verification operation prior to the visitor's access request, that the on-line service has a different second level of the security status, it causes the web page object to have different second contents, and thereby automatically controls the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined and changed web page object contents when the visitor requests access to the on-line service, and

wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed by the verification service prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line

service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein when the verification service causes the web page object to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser.

2. **(Currently Amended)** An apparatus according to claim 1, ~~wherein the on-line service comprises devices and services, and~~ wherein the verification service determines the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

3-8. (Canceled)

9. (Previously Presented) An apparatus according to claim 2, wherein the verification service periodically receives results of a new vulnerability scan of the devices and services comprising the on-line service and causes the contents of the web page object to be changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

10-20. (Canceled)

21. **(Currently Amended)** A method for providing a security status of an on-line service, comprising:

hosting a web page object separately from one or more web pages of the on-line service;

providing a link to the web page object so that it is automatically rendered by a browser when a visitor uses the browser to access the one or more web pages of the on-line service via a public network;

providing an indication of the security status of the on-line service to the visitor via the automatic rendering of the web page object by the visitor's browser, wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status; and

changing the contents of the web page object to be automatically rendered and displayed in accordance with a determination of a level of the security status, including:

in a first verification operation prior to the visitor's access request, causing the web page object to have first contents if the on-line service has a first level of the security status, and

in a second verification operation prior to the visitor's access request, causing the web page object to have different second contents if the on-line service has a different second level of the security status,

thereby automatically controlling the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined web page object contents when the visitor requests access to the on-line service,

wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein, when the web page object is caused to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser.

22. (Previously Presented) A method according to claim 21, wherein at least one of the first and second verification operations includes scanning the on-line service from a remote address on the network.

23-26. (Canceled)

27. **(Currently Amended)** A method according to claim 21, ~~wherein the on-line service comprises devices and services, and~~ wherein the first and second verification operations include determining the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

28. (Previously Presented) A method according to claim 27, further comprising periodically receiving results of a new vulnerability scan of the devices and services comprising the on-line service and causing the contents of the web page object to be changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

29. (Previously Presented) A method according to claim 21, wherein the web page object comprises an image and an associated URL.

30. (Previously Presented) A method according to claim 21, wherein the web page object comprises a graphical file whose contents are periodically updated in accordance with a periodically determined security status level.

31. (New) A method comprising:

scanning a first on-line service via the public Internet to determine potentially vulnerable devices and services comprising the first on-line service, the first on-line service having a publicly accessible first website at a first IP address;

scanning a second on-line service via the public Internet to determine potentially vulnerable devices and services comprising the second on-line service, the second on-line service having a publicly accessible second website at a second IP address;

storing respective lists of the determined devices and services of the first and second on-line services;

storing respective web page objects for the first and second on-line services;

making the web page objects accessible on the public Internet via IP addresses that are unrelated to the first and second IP addresses of the first and second websites;

identifying a list of potential vulnerabilities through which hackers can gain unauthorized access to devices and services of on-line services;

using the vulnerabilities list to determine security status levels of the first and second on-line services;

controlling contents of the stored web page objects of the first and second on-line services in accordance with the determined security status levels;

providing access, when a first visitor accesses the first website via the public Internet at the first IP address, to the web page object of the first on-line service, and thereby automatically providing the first visitor with the determined security status level of the first on-line service when the web page object is retrieved from the unrelated IP address and rendered by a browser used by the first visitor; and

providing access, when a second visitor accesses the second website via the public Internet, to the web page object of the second on-line service, and thereby automatically providing the second visitor with the determined security status level of the second on-line service when the web page object is retrieved from the unrelated IP address and rendered by a browser used by the second visitor,

wherein, when the contents of the web page object of the first and second on-line services is controlled in accordance with certain of the determined security status levels, the web page object appears invisible to the first and second visitor after it is rendered by the first and second visitors' browser.

32. (New) A method according to claim 31, wherein the step of using the vulnerabilities list includes running vulnerability test scripts against the devices and services of the first and second on-line services via the public Internet.

33. (New) A method according to claim 31, wherein the step of using the vulnerabilities list includes comparing a fingerprint of a vulnerability against the stored lists of devices and services of the first and second on-line services.